FBI - Feature # 1862: Fail-Safe Switch to prevent runaway blocking

Status:	Closed	**Priority:**	Immediate
Author:	Lauri Carpenter	**Category:**	
Created:	09/16/2011	**Assigned to:**	Lauri Carpenter
Updated:	10/25/2011	**Due date:**	
Subject:	Fail-Safe Switch to prevent runaway blocking		

Description: <pre>

We have a preliminary fail-safe design algorithm (outlined in
pseudo-code below). One question on requirements remains. We
are waiting for an answer from Joe.

FBI Fail-Safe Switch Requirements
==========
A fail-safe mechanism must be in place to prevent out-of-control
blocking.

Requirements that we have already discussed and agreed to:

- must go into effect to disable blocking when a THRESHOLD_COUNT per
  THRESHOLD_TIME_PERIOD threshold has been exceeded
- must go into effect automatically (that is, not require human
  intervention to turn off blocking)
- must be reset by a human in order to restore blocking once
  the fail-safe has been triggered (i.e., NOT a throttle to
  slow things down, but an actual ON/OFF switch that is turned
  OFF internally to the software and turned back ON by human)
- FBI Administrator should have control of both the THRESHOLD_COUNT and
  the THRESHOLD_TIME_PERIOD settings (i.e., they must BOTH be configurable)
- block requests do NOT need to be requeued, they can just fail
  with a recognizable "threshold exceeded" exception
- no such fail-safe is required for UNBLOCK requests.
- the design should be forward thinking enough to recognize
  that there may be different thresholds for different block
  scopes (i.e., border blocking may have a different threshold
  than "default" blocking)

Requirements that we suspect are A Good Thing but you have not approved:

- there should be an additional flag (send_email_when_threshold_exceeded_flag)
  to determine if email should be sent when threshold is exceeded.
- the address to whom such email should be send should be configurable
  (threshold_exceeded_email_address)
- there should be an additional THRESHOLD_WARN level (with appropriate
  data validation) and send_email_when_warn_exceeded_flag, to send an email
  message when the warning level is reached (so that a person can raise
  the threshold in time when lots of blocking activity is legitimately
  required)

REMAINING QUESTION:

- do we need to persist a blockRequest artifact in the FBI database when the request is rejected because blocking is disabled due to threshold exceeded?
  - o much easier NOT to persist the requests that occur after blocking has been disabled due to threshold exceeded
  - o TIssue client has its own logging and will have artifacts
  - o (other clients may not)
  - o apache URL logging and/or django call timing may provide an easier-to-implement alternative without cluttering the blockRequest table with failed requests

==========
==

PSEUDO-CODE FailSafeSwitch:

The FailSafeSwitch is a singleton with ONE method: getToken.
The getToken method either returns successfully, or it raises
a ThresholdExceeded exception.

FailSafeControls table contains:

```
block_scope_code    # foreign key into block_scopes
threshold_count
threshold_warn
threshold_minutes
threshold_updated_by_actor
threshold_update_date
threshold_exceeded_flag
token_count
token_fill_date
send_exceeded_email_flag
send_warning_email_flag
email_contact_address
```

```
def getToken(block_scope_code):
    # read db record for this block_scope_code;
    #  if none, read db record for DEFAULT block_scope_code

    # already disabled?
    if threshold_exceeded_flag:
        # ALREADY DISABLED, abort with exception.
        raise ThresholdExceeded()

    # refill check:
    if token_fill_date + threshold_minutes <= now:
        # fill the bucket
        token_count = threshold_count
        token_fill_date = now
        save()

    # threshold check:
    if token_count <= 0:
```

```
            # bucket is empty: DISABLE BLOCKING
            threshold_exceeded_flag = true
            threshold_exceeded_date = now
            save()
            if send_exceeded_email_flag: send_threshold_exceeded_email(to=email_contact_address)
            raise ThresholdExceeded()

          else:
            # take one from the bucket
            token_count -= 1
            save()
            return

        </pre>
```

History

09/21/2011 08:42 am - Lauri Carpenter

- Status changed from Assigned to Resolved

- % Done changed from 0 to 100

<pre>
Requires new v2_1a releases of:
  - ncis_common (for makefile changes)
  - fbi_db, fbi_db_models (for new request_timings table, which implements the archeological
    artifacts when/if blocking goes amok
  - fbi_core (which contains the core logic for FailSafeSwitch and its configuration and usage)
  - fbi_gui (which exposes the maintenance pages to fbi admins)
</pre>

10/25/2011 02:30 pm - Randy Reitz

- Status changed from Resolved to Closed